CONFIDENTIAL

(U) DEPARTMENT OF STATE CLASSIFICATION GUIDE (DSCG 11-01)

May 2011, Edition 1

CONFIDENTIAL

Classified by: Under Secretary for Management, Patrick Kennedy.
Reason: 1.4(c), (d)
Declassify On: 05/20/2036

TABLE OF CONTENTS

(U) DEPARTMENT OF STATE CLASSIFICATION GUIDE (DSCG)

A GUIDE FOR THE CLASSIFICATION OF DOCUMENTS
UNDER EXECUTIVE ORDER 13526

I. INTRODUCTION AND BACKGROUND

(U) A. Name and Citation

(U) This Guide is entitled *Department of State Classification Guide, 2011, Edition 1.* It is abbreviated DSCG 11-01. The abbreviated title shall be used when citing the Guide in classification actions. When the Guide undergoes major revision, this shall be indicated in the title by the year in which it occurs. Lesser changes shall be indicated by a change to the number following the year. For instance, the first change to this Guide would change the abbreviated title to DSCG 11-02. The second change would result in DSCG 11-03, etc.

(U) B. Purpose and Scope

(U) This Classification Guide replaces DSCG 05-01 and is for the use of State Department employees in classifying information they create or control under the terms of Executive Order 13526, which was issued to replace E.O.12958 on December 27, 2009 and became fully effective on June 27, 2010. This Guide constitutes the classification authority to be cited by persons without original classification authority (OCA) and should be used also by persons with OCA when the Guide properly describes and characterizes the information to be classified. Documents that are classified using this Guide are derivatively classified under its authority. This Guide does not affect the authority and procedures for classifying derivatively from other documents. This Guide provides the authority for the classification of national security information that it describes but the exercise of judgment by users is required as to the need for, level, and duration of classification. For purposes of contractor compliance with national-level safeguarding directives, this Guide is a compliance document for State Department contractors.

(U) This Guide describes the type of information most often classified at Foreign Service posts abroad and in Department of State domestic offices. This Guide is designed to be as specific as possible but flexible enough to cover most situations requiring the classification of information. The classifier must seek the authority of an OCA to classify information not covered by this guide that requires classification protection.

(U) Sensitive But Unclassified and Controlled Unclassified Infomation. This Guide concerns only classification; it does not address information that does not meet the criteria for classification on national security or foreign affairs grounds but which may require protection for other reasons such as personnel and other privacy protected information, trade secrets and confidential commercial information, deliberative process law enforcement, etc. Neither SBU nor CUI is a security classification and does not protect national security information from unauthorized disclosure.

(U) Supplemental Guidance. Bureaus may supplement this Guide with additional guidance tailored to their specific geographical or functional responsibilities, and/or covering aspects of E.O. 13526 not covered in this Guide. This Guide does not cover, for instance, issues relating to Special Compartmented Information (SCI) including codeword or special access. All such supplemental guidance must be cleared with the Office of Information Programs and Services (A/GIS/IPS), which has overall responsibility for classification guides within the Department. A/GIS/IPS will review such guides to ensure that they are consistent with this Guide and will coordinate, as appropriate, with other concerned agencies and, as required, obtain the clearance of the Information Security Oversight Office (ISOO), which has government-wide responsibility for implementation of E.O. 13526. Nothing in this Guide is intended to preclude elaboration of E.O. 13526 and the ISOO Implementing Directive as they apply to the specific requirements and responsibilities of individual bureaus in the Department. Guides in effect at the time of issuance of this Guide remain in effect without amendment. Copies of any existing guides that have not already been forwarded should be sent to A/GIS/IPS which maintains a central record of department guides.

(U) C. Definitions and Authorities from E.O. 13526

1. (U) Classification Levels. (U) Section 1.2(a) of E.O. 13526 defines, unchanged from the previous order, the three levels at which information may be classified:

> *(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.*
> *(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.*
> *(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.*

(U) Language from the original iteration of E.O. 12958 that was dropped in the 2003 amendments has been restored to this E.O. Section 1.2(c) states that "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level."

2. (U) Damage to National Security. The definition of "Damage to the national security" is contained in Section 6.1(l) of E.O. 13526. Note that the language specifically equates harm to the foreign relations of the United States with damage to the national security:

"Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

3. (U) Classification Prohibitions and Limitations. E.O. 13526, Section 1.7(a), states that:

In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

1) conceal violations of law, inefficiency, or administrative error;
2) prevent embarrassment to a person, organization or agency;
3) restrain competition; or
4) prevent or delay the release of information that does not require protection in the interest of the national security.

(U) Section 1.7(b) states that "Basic scientific research information not clearly related to the national security shall not be classified."

(U) Section 1.7(c) specifies that information that has been released to the public under proper authority may not be reclassified unless the action is personally approved in writing by the agency head and unless it may be reasonably recovered without bringing undue attention to the information. Additionally, there are reporting requirements and specific procedures for information in the legal custody of the National Archives.

(U) Section 1.7(d) specifies that after information has been requested under the Freedom of Information Act (FOIA), the Privacy Act, or the access provisions of this order, it can only be classified or reclassified under the direction of the Secretary, Deputy Secretary or Under Secretary for Management (M). This procedure is intended to ensure that classification is not used inappropriately to keep information from the public after it has been requested. M has directed by Notice published in the Federal Register that the authority to take such action be exercised by the Deputy Assistant Secretary for Global Information Services. Holders of information that requires classification in these circumstances should contact the Office of Information Programs and Services (A/GIS/IPS).

4. (U) Classification Categories

(U) ***Section. 1.4. Classification Categories.***
Information shall not be considered for classification unless it concerns:
(a) military plans, weapons systems, or operations;
(b) foreign government information;
(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;
(f) United States Government programs for safeguarding nuclear materials or facilities;
(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
(h) the development, production or use of weapons of mass destruction.

(U) II. ORGANIZATION AND USE OF THE GUIDE

(U) The categories of information that may be classified are enumerated in Sections 1.4(a) through (h) of Executive Order 13526 quoted verbatim above, and they are repeated in slightly abbreviated form at the beginning of Part IV below as the subparagraph headings for that part of the Guide. They are followed by the correct citations from E.O. 13526, i.e. "Foreign Government Information" by "1.4(b)".

(U) Part IV of this Guide is a discussion of the application of these classification categories to information in documents created by Department of State personnel. Most State Department documents are classified because they contain foreign government information, discuss foreign relations, or identify confidential sources, and are classified under E.O. 13526 Sections 1.4(b) and 1.4(d). These categories are discussed in considerable detail in Sections IV B and IV D respectively. Some categories of classified information in State-created documents will have been originally classified by another federal agency, e.g., military plans by a DOD component, intelligence by CIA or other intelligence agency, etc. This is particularly true for INR, which produces many all-source documents drawing on material from other agencies. In these cases, the other-agency-derived information should be given a derivative classification in the State document. The discussion of categories of information usually classified derivatively is, therefore shorter in this Guide. Bureaus and offices in the Department that rely extensively on derivative classification may supplement this guide with their own guide.

(U) Classifiers should cite all the classification categories that apply to a document. As will be evident in the descriptions of classification categories in Section IV of this Guide, multiple categories of Section 1.4 of E.O. 13526 may apply to a single document. For instance, information passed by a foreign government in the course of negotiations for an agreement on exchange of scientific information to be used in protecting facilities against international terrorism could be protected under three, and possibly four, categories, i.e. 1.4(b), 1.4(d), 1.4(e) and possibly 1.4(g). Applying all that are applicable will help ensure the level and type of protection required, as well as help determine disposition in the event of a request for declassification and release of the information.

(U) In Part IV each classification category is described generically, usually followed by illustrative examples that are not intended to be comprehensive. An effort to include in this Guide every possible contingency would produce an unmanageably cumbersome product with an unacceptably short shelf life. Essential to the use of this Guide is the understanding that its effective use requires application of the knowledge,

experience and, especially, judgment of the classifier. State Department personnel are expected, for instance, to appreciate the cultural differences that might make a type of information that is of little concern in one country potentially explosive in another.

(U) When State Department information not described in this Guide requires classification protection, it must be classified by an OCA.

(U) **III. Duration of Classification** (U)

1. Declassification Date or Exemption Required. Every classification action, whether made by an OCA or using this guide or other derivative source, must be accompanied by a declassification date or event or by a citation exempting the information from automatic declassification. Suggested durations for classification are contained under the discussion of each category of information in Part IV below.

2. Shorter is Preferred. Information covered by the classification categories of Section 1.4 may be classified for up to 25 years at the time of classification. (See below for the exceptions to the 25 year limitation.) Notwithstanding the authority to classify for longer, E.O. 13526 carries over a bias in favor of a date or event not greater than 10 years. Section 1.5(b) states:

> *If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for classification for up to 25 years from the date of the original decision.*

3. Picking a Date. A significant amount of State Department information will be adequately protected by assigning a classification duration of ten years or less, but that duration of classification could be grossly inadequate for many classes of information. This is particularly true for information derived from foreign governments and confidential sources but also, as described in Part IV, for a number of other types of information as well. Often there are multiple considerations in determining the duration of classification. For example, the information provided by a source may be of lessened sensitivity in ten years, but the fact that the source provided the information could be sensitive for as long as the source lives. Similarly, the signing of an agreement generally means that much of the related information loses its sensitivity, but a negotiating history of the agreement describing the diplomatic details and discussions could well remain sensitive for many years. It is therefore incumbent upon the user of this guide, as for OCAs, carefully to consider each duration decision.

4. Exceptions to the 25 Year Limit. E.O. 13526 does not authorize original classification beyond 25 years except to protect three specific categories of information: information that should clearly and demonstrably be expected to reveal the identity of a confidential human source, or human intelligence source, or key design concepts of weapons of mass

destruction. The Information Security Oversight Office (ISOO) Directive implementing E.O. 13526 states that documents containing information revealing confidential human sources or human intelligence sources shall have a classification duration up to 75 years and shall be marked "50X1-HUM." Information revealing key design concepts of weapons of mass destruction shall also have a classification duration up to 75 years and shall be marked "50X2-WMD".

5. Exempting from Automatic Declassification at 25 Years. Because most information may not originally be classified for more than 25 years does not mean that it cannot be classified for as long as it requires protection. Before any classified information is released to the public or retired to the National Archives, it will be reviewed to determine if it must continue to have classification protection. For most information this extension of classification protection will normally take place as a result of the systematic review conducted pursuant to Section 3.3 of E.O. 13526. This review is generally conducted as the 25-year declassification deadline nears, in sufficient time to ensure that still-sensitive information does not become automatically declassified. The categories of information that may be exempted from automatic declassification at 25 years are enumerated in Section 3.3(b) of E.O. 13526. That section of the Order is reproduced as Annex B to this Guide.

6. Using an Event Instead of a Date. It is sometimes possible and useful to designate an event for automatic declassification. This should only be done, however, when the event is reasonably definite and foreseeable. The event cannot be more than 25 years away. Examples where an event might usefully be used could include:

-- Upon signing of the treaty;
-- After the spring 2012 NATO Ministerial;
-- After the Secretary's scheduled March 2012 presentation at the UNSC; and
-- When the minutes of the meeting have been approved and published.

An indefinite or hypothetical event should NOT be used for declassification. Examples of incorrect usage would include:

-- When the issue is no longer sensitive;
-- When any party to the talks divulges their content; and
-- When countries X and Y improve relations.

IV DESCRIPTIVE CLASSICATION AUTHORITY BY CATEGORY

(U) Order of Discussion of Classification Categories

(U) A. MILITARY PLANS, WEAPONS SYSTEMS, OR OPERATIONS. [1.4(a)]

(U) Information in this category might include: military plans for operations or contingencies, scientific or engineering analyses or descriptions of U.S. weapons systems; weaknesses in the current U.S. defense posture; U.S. national and military command, control and communications systems, and nuclear weapon release authority and agreements, and any other information likely to weaken U.S. weapons systems. State Department officials have extensive involvement in various national and international military organizations and operations and therefore create numerous documents containing classified information relating to military plans, weapons systems or operations. Virtually by definition, however, classified information in this category is likely to have originated at DOD or one of the armed services. When this is the case, the document should be classified derivatively based on the original classification reason, level and duration. When a State Department official creates information that has not previously been classified, as for instance, a proposal for military response to a particular threat or action, or an analysis of foreign reaction to U.S. military action, the information should be classified SECRET (though CONFIDENTIAL may in some circumstances be adequate) for at least ten and possibly as long as 25 years. If there is question as to the need for, level or duration of classification, classification action should be taken by an OCA familiar with the subject matter.

(U) B. FOREIGN GOVERNMENT INFORMATION [1.4(b)]

(U) **1. Bases for Classifying Foreign Government Information (FGI).** The bases for classifying FGI are found in several other parts of the E.O. in addition to Section 1.4(b).

FGI is defined in Section 6.1(s) of E.O. 13526 as:

> *(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;*
> *(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or*

(3) information received and treated as "foreign government information" under the terms of a predecessor order.

Note that under this definition information is considered FGI if it is received from "an organization of governments." This includes, of course, NATO, the UN and its dependent organizations such as the U.N. High Commission for Refugees, but would not include the International Committee of the Red Cross (ICRC) or similar organizations composed in whole or part of non-governmental groups. This can be significant in view of Section 1.1(d) which states that:

"The unauthorized disclosure of foreign government information is presumed to cause damage to the national security."

Thus the unauthorized release of information from the ICRC or similar organizations would not benefit from the presumption of harm but may be protected under Section 1.4(d), described below in IV D.

"Damage to the national security" is defined in Section 6.1(l) as *"harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility and provenance of that information"*. (Underlining added.)

Taken together these provisions constitute authority, as described below, for classifying a range information including, for instance, information from a foreign government that would not normally be classified were it of U.S. origin.

(U) 2. General. Observing the confidentiality of the exchange of information between governments is a basic requisite for the successful conduct of diplomacy since trust in the discretion of the other side is often essential to successful negotiations and discussions. The expectation of confidentiality applies equally to exchanges between adversaries and friends. Actions that undermine this trust carry costs which must be weighed. Additionally, foreign governments are the frequent sources of information vital to the formulation and execution of U.S. foreign policies. The continued access to this information will generally depend upon our willingness to protect such information and the foreign government as the source. The same may be true of certain exchanges with officials of international organizations and other confidential international organization material.

(U) Foreign-derived information is often itself sensitive and the need for classification will be clear based upon its substance. This will not always be the case, however, so the classifier must calculate the likely reaction of the source government to disclosure, even if the information is not by itself sensitive, and weigh the effect of that reaction on U.S. foreign affairs interests, including the willingness of the government or official to share information in the future. Some governments are more protective of their information than are others – including even the fact that they have provided

information to the U.S. at all. Some governments insist that their information be protected for a set period of time, such as 25 years. In deciding whether to classify, the classifier may conclude that a predictable negative reaction of the originating country to release of its information is of sufficient magnitude to justify classification even in the absence of self-evident sensitivity of the information itself.

(U) If a foreign government or international organization of governments has classified the document at a level which corresponds to the U.S. classification "Confidential" or above, the document should be considered properly classified and given protection at least equivalent to the comparable U.S. classification. A U.S. classification may be assigned, but there is no need to do so if the receiving agency determines that the foreign government markings are adequate to meet the purpose served by U.S. classification markings. [Section 1.6(e)]

(U) Classifying FGI after the fact. Certain types of information exchanged with foreign governments (e.g. dealing with protocol, administrative and consular matters) are not normally classified by either government, though both parties may regard them as privileged communications that should not be made public. The fact that FGI is not classified at time of receipt does not mean that it would necessarily be released in response to a Freedom of Information Act or other access request. Under procedures for processing such information requests, a determination would be made at the time of the access request whether foreign relations considerations might require withholding from release and, if necessary, whether the document should be classified at that time under the provisions of Section 1.7(d) of E.O. 13526. It is clearly preferable, when the potential damage to national security is evident, that the information be classified from the beginning.

(U) 3. Types of FGI Likely to Require Classification. FGI can encompass a broad range of types of information, including:

(U) a. High Level Correspondence. This includes letters, diplomatic notes or memoranda or other reports of telephone or face-to-face conversations involving foreign chiefs of state or government, cabinet-level officials or comparable level figures. (See Part IV D below for the classification of information from non-governmental figures such as leaders of opposition parties.) It should be presumed that this type of information should be classified at least CONFIDENTIAL, though the actual level of classification will depend upon the sensitivity of the contained information and classification normally assigned by the U.S. to this category of information. Information from senior officials shall normally be assigned a classification duration of at least ten years. Some subjects, such as cooperation on matters affecting third countries, or negotiation of secret agreements, would merit original classification for up to 25 years.

(U) b. Foreign Government Documents on Matters of Substance. These include, but are not necessarily limited to, foreign government diplomatic notes, aides-memoir, position papers, "non-papers" and USG transcriptions of foreign documents, e.g. the telegraphic reporting by a U.S. embassy of the text of a foreign government document.

Foreign government documents will frequently bear no classification markings when received. Whether the information should be classified will depend upon the sensitivity of the underlying subject to both governments. As a general rule, such FGI should be classified at the highest level normally assigned to this kind of information by either government and for the same length of time as U.S. documents containing similar information. When there is no comparable U.S. information to provide a guide for duration, the FGI should normally be classified for ten years from date of origin.

1.4(C)
1.4(D)

d. (U) Foreign Government Information Classified By Agreement. The United States has entered into agreements with a number of other countries that provide for the protection of defined types of classified information. These agreements (which go by various names but are often called General Security of Information Agreements – GSOIAs) generally specify the conditions under which information originated by the

parties may be released to other parties or the public. Where such agreements exist, the USG is bound by them. Additionally, the United States, as a member of a number of current and former organizations, is bound by agreements governing the handling and release of the documents of those organizations. Information that falls in these categories should be classified at the level and for the duration specified by the relevant agreement.

(e) Confidential/Modified Handling Authorized. If the U.S. and the party providing the information mutually agree, FGI may be stored and handled under conditions less rigorous than that required for U.S. Confidential. Under the definition of FGI cited above, U.S. origin information may also be considered as FGI for purposes of this lower standard of handling: ["*(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments ... requiring that the information, the arrangement, or both, are to be held in confidence*"] This procedure is most common in negotiating situations where the parties wish to preserve the confidentiality of the proceedings and are willing to accept lower standards of security for handling, stowage and transmission. It has also been adopted for longer term arrangements. This requires that the parties agree on the standards to be applied and formalize them in an agreement, exchange of notes, agreed minute or by any other unambiguous means. Before the U.S. party enters into any such agreement, it should seek the procedural guidance of DS and A/GIS/IPS and the approval of L.

(U) C. INTELLIGENCE ACTIVITIES (INCLUDING COVERT ACTIVITIES), INTELLIGENCE SOURCES OR METHODS, OR CRYPTOLOGY [1.4(c)]

(U) What constitutes an intelligence source or method is defined by the Director of National Intelligence. Generally, information concerning intelligence activities and programs, including signals intelligence and other technical collection efforts, will have been classified originally by the CIA or another intelligence agency or, in the case of cryptologic information, by the National Security Agency (NSA). When this is the case, the document should be classified derivatively based on the original classification reason, level and duration. When the document is derived from sources marked as exempt from automatic declassification at 25 years (i.e., 25X1 through 9) the derivative classifier will carry forward all such markings from the sources. When the document being created and classified contains information about a human intelligence source, it should be marked "50X1-HUM" indicating that because of its sensitivity it has been exempted at origin from automatic declassification at 50 years. (See also IV D 7, below, on Confidential Human Source.)

(U) Often a purely State Department document will include reference to an intelligence presence in a particular country. This may be in the form of information from or about an intelligence source or simply identification of a U.S. intelligence presence. A document containing such information should be classified at least CONFIDENTIAL for a duration of 25 years.

(U) Roger Channel messages are controlled by the Assistant Secretary, INR. They are used to report sensitive intelligence matters and have very limited distribution.

Roger Channel should normally be classified SECRET for a duration of 25 years, or marked 50X1-HUM if they reveal the identity of a human intelligence source. (Inclusion of information here about Roger Channel does not constitute authority to initiate messages in this channel. This will normally be done by an OCA.)

(U) Cryptologic materials are generally held by the Department on a temporary basis. Cryptologic materials come under the control of the National Security Agency (NSA) and classification determination will generally have been made by that agency. These might include information on: U.S. cryptologic capabilities and vulnerabilities; foreign cryptologic capabilities and vulnerabilities; cryptoperiod dates; and inventory reports of COMSEC material. When there is question about the classification of possible cryptologic information, it should be given to officials in the Department who regularly deal with such information or sent to NSA for a classification determination. In the interim, it should be marked and treated as TOP SECRET/SCI with a duration of 25 years. If storage is not available at the TS/SCI level, while a classification determination is pending it should be marked and treated in the interim as TOP SECRET, but in no event as less than SECRET.

(U) D. FOREIGN RELATIONS OR FOREIGN ACTIVITIES OF THE UNITED STATES INCLUDING CONFIDENTIAL SOURCES [1.4(d)]

(U) As outlined in this Part, the conduct of foreign affairs takes place in a highly fluid and often rapidly changing environment. The sensitivity of certain types of information as well as the duration of that sensitivity may vary from country to country. This Guide describes below the most common circumstances in which information will require classification to avoid damage to U.S. foreign relations or U.S. diplomatic activity. These should cover, at least by logical extension, most circumstances where information will require classification. The discussion below focuses on foreign countries, but also applies to international organizations where the same considerations apply.

(U) 1. Sensitive Diplomatic Commentary, Reporting and Analysis.

(U) General Considerations. Reporting on and analysis of the internal affairs or foreign relations of a country is a central function of U.S. foreign service posts and is vital to the formulation and execution of U.S. foreign policy. This reporting should be unclassified when the subject matter is routine, already in the public domain, or otherwise not sensitive. Drafters will sometimes find it preferable to leave out or separately report sensitive information in order to obtain the broadest useful dissemination of the remaining reported information. However, much reporting and analysis necessarily contains material that, if released, would damage U.S. relations with the government or important elements of a country or otherwise undermine U.S interests and should be classified. This could include:

(U) **a.** Reporting and Analysis about the policies of the government, or a political party, or social or economic group. Sensitive commentary in this category warranting classification can be either favorable or unfavorable. The basic question is whether

release of the information would complicate U.S. political activities or impair relations. For example, favorable commentary about the policies of opposition parties or personalities could complicate relations with the government. Even neutral commentary could have a negative impact if it gives the impression that the USG is too deeply involved in the country's affairs. However, neutral commentary about a country's current domestic or foreign affairs is unlikely to be very sensitive and therefore may not require a long duration of classification. Classification at the CONFIDENTIAL level for a duration of ten years or less is likely to be adequate for this type of information. (But see Section IV.D 7 below when information identifies or is derived from a confidential human source.)

(U) When the commentary is negative, the information is inherently more sensitive and likely to require a higher level and longer duration of classification. This could include any kind of negative commentary, whether based on policies or personalities. Especially sensitive examples of negative commentary might include reports of corruption of individual officials, foreign government agencies or other institutions. When assigning classification duration, classifiers need to take into account the frequency with which foreign political, economic, religious and social leaders survive adverse circumstances to rebound and again become significant players on the political or diplomatic scene.

(U) The Bureau of Intelligence and Research (INR) produces a broad range of all-source analyses and coordinates intelligence policy. Most of these reports are derivatively classified from sensitive sources. Where INR reporting cables or other documents are based upon State or unclassified sources, classification will be determined, as appropriate, by this Guide, supplemental guidance such as that referenced in section 1.B., or guidance issued by the Director of National Intelligence. See also Section C on Intelligence Activities.

1.4(C)
1.4(D)

1.4(C)
1.4(D)

(U) The level of classification given to policy documents will depend upon the sensitivity of the underlying issues, but a classification of SECRET will often be appropriate. (In rare circumstances where the release of policy deliberations could result in exceptionally grave damage to the national security, a TOP SECRET classification might be appropriate. In these cases, the classification should be derived from an existing TS document, or an OCA with TS authority should be asked to classify the information. If codeword or compartmented information is indicated or implied in the policy document, INR should be asked to classify the information.) Policy information may also remain sensitive for a considerable period of time. The fact that a particular policy was not adopted or is no longer in effect will not necessarily diminish the sensitivity of the policy deliberations. Such information should generally be protected for at least ten years; depending on the circumstances, a period of 25 years could be appropriate.

(U) b. Contingency Plans. The policy process frequently culminates in specific plans for dealing with various actual or potential situations. Many of the same sensibilities described above in relation to the policy debate would probably be embedded in the resulting plan, whether or not it has been implemented, and similar consideration should be given to classifying the information at the SECRET level (and in rare circumstances at the TOP SECRET level) and for a duration of ten or more years. Additionally, references to older contingency plans which remain in effect or which are relevant to current situations or plans should be considered for classification.

1.4(C)
1.4(D)

(U) 4. U.S. Involvement in International Disputes

(U) Because of its great power status there are few international disputes or controversies in which the U.S. does not have an interest, either directly as a party, because a friend or ally is a party, or because of the U.S.'s actual or potential role as mediator or participant in conflict resolution efforts. This includes new controversies but also may include issues which date back many years (or decades) that are still the subject of current negotiations, ongoing dispute, open or hidden resentments, current or potential irredentism, or capable of again becoming contentious issues involving U.S. interests. In those cases where the U.S. has been, or may again be, involved as an intermediary, it is an additional concern that information not be released which would prejudice future negotiations on unresolved issues or impair the U.S.'s ability to continue an intermediary role to resolve those issues. For this reason, it is important that information be classified when its release might cause or revive conflict or controversy, inflame emotions or otherwise prejudice U.S. interests. It may be necessary to classify information about active conflicts, but also about long-standing ones such as Israel-Palestine and India/Kashmir/Pakistan, as well as information relating to long-simmering or dormant controversies such the Falklands Islands or border disputes among Andean countries.

(U) The extent of U.S. involvement in the basic dispute or settlement efforts will often determine the potential damage to the national security and foreign relations. Where there is involvement, a classification of SECRET will frequently be appropriate. As the foregoing discussion suggests, this type of information can remain sensitive for an appreciable length of time, even well beyond the time that the dispute is supposedly "settled". It should, therefore, normally be classified for at least ten and up to 25 years.

(U) 5. Confidential Diplomatic Exchanges and Negotiating Agreements.

(U) In negotiations and other diplomatic exchanges it is a deeply rooted and long-standing tradition of diplomatic intercourse that the details of the exchanges between the parties, including commentary, will not be divulged during the course of the negotiations. Most countries expect that their diplomatic communications will be treated with confidence even after the matter under consideration is concluded. As a general rule, therefore, when negotiations or other diplomatic exchanges are conducted in a non-public, off the record, channel, details should be classified. This rule applies to negotiations and exchanges with international organizations as well as with foreign governments. Information obtained from (and in some contexts, shared with) other governments or international organizations of governments in a non-public, confidential exchange should be treated as Foreign Government Information (FGI) and classified for as long as necessary, taking into account both the inherent sensitivity of the information and the expectations of that party. (See section on FGI above.)

(U) In many cases, U.S.-origin classified information relating to the U.S. position in negotiations needs to be classified only until the negotiations have been completed. However, if the same or similar issues are to be separately negotiated with another party or parties, or if an agreement is controversial and is likely to remain a sensitive topic in the public discourse of the other negotiating party, U.S. interests may require longer-term classification of information regarding the negotiations. Additionally, references to prior international agreements that remain classified should generally be classified also.

(U) The sensitivity of the subject matter of a negotiation will dictate both the level and duration of classification. For instance, agreements on defense-related subjects such as mutual defense or force basing agreements are likely to have greater sensitivity than economic or consular agreements. Additionally, agreements on defense subjects may include provisions specifying the classification protection to be given to the negotiating record or the text of the agreement. When this is the case, those terms shall govern level and duration of classification.

(U) While there is wide agreement that successful negotiations require and justify the classification and withholding of information, there is also a strong belief that citizens have the right to be informed of the commitments the government makes on their behalf. Therefore, information on the negotiation of international agreements ought to remain classified only as long as necessary to protect U.S. interests evident at the time of the agreement. In most cases, this will mean that a duration of ten years or less should be applied unless the particular circumstances, including the terms of the agreement, require a longer duration of classification.

(U) 6. <u>Confidential Relations with Foreign Domestic Entities</u>.

	1.4(C) 1.4(D)

1.4(C)
1.4(D)

(U) Information relating to the security and protection of U.S. individuals and facilities may also be classified under Section 1.4(g). Information relating to security that does not warrant classification may nonetheless require protection and should be treated and marked as SBU (soon to be CUI). (See Section IV.G. below). Information relating to law enforcement investigative materials that does not qualify for classification protection under E.O. 13526 may, nonetheless, be properly withheld from public access under the FOIA and should be labeled SBU/CUI.

(U) 7. Confidential Human Sources

(U) A confidential human source is any individual who has provided, or who may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information, or the relationship, or both, are to be held in confidence. (This is distinct from a Human Intelligence Source covered by Section 1.4(c). See IV.C. above.) The understanding that there is to be confidentiality need not – and in fact generally will not—be explicit. It is enough that an individual under the circumstances would reasonably anticipate that his U.S. interlocutor would treat the information or the relationship as confidential. The identity of the individual and the information should not be classified in the absence of the threshold of identifiable damage to the national security, but this determination need not focus on the specific individual or information at hand if just divulging the source would be likely to damage confidence in the willingness of the U.S. to protect sources of information passed in the expectation of confidentiality.

1.4(C)
1.4(D)

(U) Classification at the CONFIDENTIAL level will generally be adequate to protect information identifying a confidential source. However, when the information being provided by the source is itself very sensitive and valuable to the U.S. or if revealing the identity of the source could result in danger to his own or to his family's life, physical well-being or livelihood, a SECRET classification would be appropriate.

(U) Special attention needs to be paid to the duration of classification of information that would reveal the identity of a confidential human source, including consideration of the possibility of negative action against the source. The duration of classification should be sufficiently long to protect the source from the danger of retribution for as long as he is alive, and longer if there is danger of retribution against his family. While classification duration of 25 years, or even less, may be adequate to protect a confidential human source in some cases, classifiers should err on the side of protection. E.O. 13526 authorizes at time of origin the exemption from automatic declassification at 50 years of information that would reveal a confidential human source or human intelligence source. In this case 50X1-HUM should be entered on the declassification date line. No other date is required.

(U) E. SCIENTIFIC, TECHNOLOGICAL, OR ECONOMIC MATTERS. [1.4(e), 1.4(d)]

(U) Section 1.4(e) authorizes classification of "scientific, technological, or economic matters relating to the national security." (Note that Section 1.7(b) of E.O. 13526 states that "Basic scientific research information not clearly related to the national security shall not be classified.") State Department personnel will often create documents containing scientific or technical information requiring classification but that

information will often already have been classified in a source document. A document creator in these cases should derivatively apply the appropriate classification level and duration from the source documents.

(U) Officials in the Department or abroad will more often make original compilations or analyses of economic matters that require classification. This could include, for instance, analyses of foreign economies or economic sectors, or of the activities of U.S. firms in foreign countries, the release of which would harm economic relations with the country or relatively disadvantage aspects of the U.S. economy. Information classified under this category might, in many instances, also be classified under 1.4(d) as relating to the foreign relations or foreign activities of the U.S. For instance, information or analysis compiled or prepared in connection with the negotiation of an international economic agreement could be classified under both 1.4(d) and (e) if release would harm the U.S. negotiating position. In some cases merely revealing the extent and depth of USG knowledge of aspects of a foreign economy could be harmful to U.S. foreign and economic relations. If more than one category of Section 1.4 applies to the same information, all applicable categories should be cited. Generally classification at the CONFIDENTIAL level will provide adequate protection to economic information, but if the information appears to be of particular sensitivity, inherently or because of the context, it should be classified SECRET. Economic information will frequently lose its sensitivity after a particular event such as the conclusion of a negotiation, the signing of a contract or the end of a harvest season. If an event is sufficiently definite and identifiable, it should be used for classification duration. Duration of 10 years will normally be adequate to protect economic information (but keep in mind the long term need to protect confidential human or institutional sources of information).

(U) F. USG PROGRAMS FOR SAFEGUARDING NUCLEAR MATERIALS OR FACILITIES [1.4(f)]

(U) The Department of Energy (DOE) is responsible for U.S. Government programs for safeguarding nuclear facilities or materials within the U.S. Department of State officials incorporating such information in Department of State documents should classify the material derivatively based on a referenced document or DOE or Nuclear Regulatory Commission (NRC) guidance. Persons who do not have access to a guide but believe that information requires classification under this category should either obtain the assistance of a Department of State OCA knowledgeable in the subject area, or send the material without delay to the Department of Energy for a classification determination. The material should be marked as SECRET for purposes of transmission and all copies should be protected at that level pending a DOE determination.

(U) Department officials occasionally create documents containing information about the safeguarding and vulnerabilities of foreign nuclear facilities and materials or nuclear materials in international transit. Frequently the information will have been originally classified by DOE or another agency or will be covered by a DOE or other agency guide. In those cases, the information should be derivatively classified at the appropriate level. Department of State originated information about safeguarding foreign nuclear facilities or materials should normally be classified SECRET for a duration of at

least 10 and up to 25 years depending on the best estimate of how long the information is likely to remain relevant to U.S. security concerns. When written guidance is not available, it is preferable that such information be classified by an OCA familiar with the subject matter.

(U) G. VULNERABILITIES OF SYSTEMS, INSTALLATIONS AND PLANS [1.4(g)]

(U) Section 1.4(g) authorizes classification of information that concerns "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security." The current wording of this section carries over wording that was added in the March 2003 amendment to E.O. 12958. This more expansive language reflects a post 9/11 concern that the classification system be capable of adequately protecting all information concerning vulnerabilities or capabilities whose release could compromise U.S. security.

(U) Department-originated information relating to installations and infrastructures should be protected if its release could compromise the security of U.S. persons, facilities or installations. Much of the information relating to U.S. installations may be adequately safeguarded without classification through the use of the control marking SBU (soon to be CUI). However, other information will, because of its greater sensitivity and possible use to individuals and groups hostile to U.S. interests, require classification under this section. With over two hundred embassies, consulates and missions abroad, the Department has particular vulnerability and responsibility in regard to this category of information. As regards information relating specifically to the design and construction of overseas facilities, the Bureau of Diplomatic Security has issued a detailed guide entitled Security Classification Guide for Design and Construction of Overseas, Facilities. It is available from the Bureau of Diplomatic Security or through Regional Security Officers at post. Nothing in this Guide is intended to amend or change that guidance.

1.4(C)
1.4(D)

1.4(C)
1.4(D)

(U Where classification is warranted, classification at the CONFIDENTIAL level will often be adequate and most appropriate, especially when the information needs to be widely shared, particularly with other agencies where personnel clearances at the CONFIDENTIAL are common. When the sensitivity of this type of information requires, it should be classified at the SECRET level. Information in these categories should normally be classified for as long as the information is likely to remain current and sensitive, usually at least 10 years, but in some cases as long as 25 years.

(U) Frequently Department officials will incorporate another agency's information relating to these categories into Department of State documents, for instance, Secret Service information in a message on presidential travel. When this is the case, the information should be classified derivatively, based upon the other agency's classification level and duration unless the Department of State information in the document requires a greater level and duration of protection, in which case it shall be classified based upon this Guide or an OCA decision.

(U) H. WEAPONS OF MASS DESTRUCTION (WMD). [1.4(h)]

(U) Section 1.4(h) of E.O. 13526 authorizes classification of information pertaining to "the development, production, or use of weapons of mass destruction." The underlined words above indicate language that was added to the wording of the previous E.O. to clarify what information is intended be classified under it. The term weapons of mass destruction can be broadly defined as explosive, chemical, biological or radiation devices capable of causing large-scale death or injury. Rather than provide its own definition of WMD, E.O. 13526 specifically adopts the definition of 50 U.S.C. 1801(p).[1] The previous, less precise, definition had resulted in information being mistakenly classified under this section as for instance, the stationing of nuclear weapons abroad. It is now clear that information should be classified under this section to protect against

[1] 50 U.S.C. 1801(p) states: "Weapon of mass destruction means—
(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;
(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;
(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18) that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons; or
(4) any weapon device that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

proliferation to terrorist groups or other potential adversaries of a defined category of weapons, or the technical information that could be used to develop these weapons. Additionally, information that would assist a potential developer of weapons of mass destruction to evade monitoring and detection by the United States and its allies and international verification bodies such as the International Atomic Energy Agency, should be considered as assisting in the development of such weapons and be classified accordingly.

(U) It is most likely that information in this category will have been developed and originally classified by another agency. In that case, State classifiers should derivatively apply the original classification level and duration. In the event that a Department official creates a document containing such information for which there is no indication of previous classification, it should be classified CONFIDENTIAL or SECRET depending upon the classifier's best estimate of the sensitivity of the information.

(U) Duration of Classification. E.O. 13526 takes into account the fact that key design concepts of weapons of mass destruction might need protection for an extensive period of time. Therefore, this category of information (like information that would reveal the identity of a human intelligence source or a confidential human source) may be marked for exemption from automatic declassification at 50 years when classified at origin. The marking to be applied in this case is 50X2-WMD.

(U) Nuclear Weapons and Radiological Weapons. While information concerning key design concepts of nuclear and radiological weapons is clearly covered by this section of E.O 13526, it also has a special status that brings it under the Atomic Energy Act, which is administered by the Department of Energy (DOE). This status and the additional requirements it imposes on the classification and handling of information are discussed in Annex C of this Guide.

ANNEX A

(U) Marking and Procedural Requirements

NOTE: This annex covering basic marking requirements is added as a convenience for classifiers. The marking instructions here are current as of the issuance date of this guide but may not subsequently reflect the latest marking guidance. More detailed marking instructions are available on ClassNet at http://a.m.state.class/sites/gis/IPS/default.aspx. (Similar information is available through the Intranet.)

E.O. 13526, Section 1.6, requires that documents be properly marked at the time of classification. If information is classified it must be protected regardless of the medium in which it is contained. For instance, if classified information is put on a disk, the disk needs to be marked appropriately.

1. **Marking Classification by an Original Classification Authority (OCA).** When information is classified by an OCA this shall include:

a. the classification level (Confidential, Secret or Top Secret);
b. the identity, by name and position, of the OCA;
c. office of document origin if not otherwise evident from the OCA title;
d. reason for classification; and
e. declassification instructions (i.e., a date or event for declassification).

2. **Derivative Classification Using Guide**. When information is classified derivatively using this Guide, the citation of the Guide in abbreviated form as DSCG 11-01 will take the place of the OCA and office of origin. (Items (b) and (c) above.) The "reason(s)" for classification (item d above) will be indicated by adding the subsection letter or letters A through G from Part IV of this Guide where the categories of information that may be classified are described. The subsection letters in Part IV all correspond to the subsections of E.O. 13526 Section 1.4. (I.e., A corresponds to 1.4(a), military plans, weapons systems, or operations; B corresponds to 1.4(b), foreign government information; D corresponds to1.4(d), foreign relations or activities, etc.) Declassification instructions should be an event or a date 25 years or less from date of origin. (Important exceptions to the 25 year limit are described below under Duration.).

A new requirement of this executive order is that derivative classifiers be identified by name and position. This should be indicated after the (Derived from" line.

Examples of classification by guide.

Classifying for twenty years from January 5, 2011 because document contains foreign government information:

Derived from: DSCG 11-1, B
Classifier: JBJones, A/GIS/IPS
Declassify on: 20310105

Classifying for 25 years from 01/05/11 because of foreign relations and economic matters relating to national security:

Derived from: DSCG 11-1, D,E
Classifier: B. Meek, PD/FR/IP
Declassify on: 20360105

3. Derivative Classification from Classified Source. When information is classified derivatively on the basis of source documents other than the DSCG, it shall bear the same markings as in 1. and 2. above but the information for these markings shall be carried forward from the source document. The source document shall be concisely identified on the "Derived from" line. When classification is derived from multiple sources, that shall appear on the derived from line and the derivative classifier shall include a listing of the source materials on or attached to the derivatively classified document. The classification and the declassification date reason shall be as listed on the source document(s). When there are multiple source documents, the declassification date shall be that from the document with the declassification date farthest in the future.

Example:

Classified by: GDJone, W/HRG/IS
Derived from: 04Berlin00423
DECL: 20350130

ANNEX B

(U) EXEMPTION FROM AUTOMATIC DECLASSIFICATION AT 25, 50, and 75 YEARS

(U) E.O. 13526 does not permit classification of information at time of creation beyond 25 years except in the case of information that would reveal the identity of a confidential human source or human intelligence source. It does, however, make provision for the subsequent exemption from automatic declassification at 25 years of information that must be protected to prevent damage to the national security. Though this exemption may be done at any time after 20 years from date of classification, it will normally take place during systematic review prior to transfer to the National Archives for permanent safekeeping.

(U) The categories of information that may be exempted at 25 years are defined in E.O. 13526 Section 3.3(b):

> ***Sec. 3.3. Automatic Declassification.***
> *(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which could be expected to:*
>
> > *(1) reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;*
> >
> > *(2) reveal information that would assist in the development or use of weapons of mass destruction;*
> >
> > *(3) reveal information that would impair U.S. cryptologic systems or activities;*
> >
> > *(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;*
> >
> > *(5) reveal actual U.S. military war plans that remain in effect;*
> >
> > *(6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;*
> >
> > *(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect*

the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

(9) violate a statute, treaty, or international agreement.

ANNEX C

NUCLEAR INFORMATION AND THE ROLE OF THE DEPARTMENT OF ENEGRGY

(U) U.S. nuclear weapons information falls under the authority of the Department of Energy (DOE) under the terms of the Atomic Energy Act of 1954 (AEA). DOE classified information falls into three categories: a) National Security Information (NSI), which is classified under the authority of the present and previous executive orders, such as E.O. 13526; b) Restricted Data (RD); and c) Formerly Restricted Data (FRD). The criteria for classifying NSI are described in the body of this Guide. The latter two classification classes are authorized by the AEA, and are administered by DOE. RD concerns the design, manufacture or utilization of atomic weapons, the production of special nuclear material (e.g., plutonium and uranium 235), and the use of special nuclear material in the production of energy. RD is controlled by DOE alone. FRD applies to information that has been removed from the RD category after DOE and DOD have determined it relates primarily to the military use of atomic weapons and can be adequately protected as NSI. Examples of FRD include information about nuclear weapons stockpile quantities, safety and storage, and deployment -- foreign and domestic, past and present. DOE shares control of FRD with DOD.

(U) RD and FRD. Department officials do not have the authority to classify information as RD under the Atomic Energy Act. Information identified as RD should be sent to DOE for classification. In the interim, it should be handled as NSI SECRET, unless marked with a higher classification. Information that is FRD should be marked as FRD and be given an NSI classification of SECRET with a classification duration of 25 years. Some records containing FRD information have previously been released to the public. The fact that the same or similar information has been previously released does not automatically mean that the FRD should not now be classified. There is currently active interagency discussion on what information should remain covered by the FRD label. It is likely that new guidelines will be promulgated that will shift much of what is now FRD to the NSI-only category. Nothing in E.O. 13526 supersedes any requirement of the AEA with regard to classification.